WHAT IS CLAIMED IS

1. A method for making an electronic exchange of an image obtained by working an original image of written information read out of a recording medium between a data transmission side and a data reception side via a network, said method comprising:

a data transmission step on said data transmission side; and

a data reception step on said data reception side;

said data transmission step including:

a first step of working said original image so as to produce worked data;

a second step of applying a digital signature to said original image so as to produce first signed data;

a third step of ciphering said first signed data with a private key of said data reception side so as to produce a ciphered signed data;

a fourth step of merging said worked data and said first signed data, applying a one-way function to obtained merged data, and ciphering an output of said one-way function with a secret key of said data transmission side so as to obtain second signed data; and

a fifth step of transmitting said worked data, said second signed data and said ciphered signed data to said data reception side;

said data reception step including:

a sixth step of obtaining said worked data, said second signed data and said ciphered signed data;

a seventh step of enciphering said obtained ciphered signed data with a secret key of said data reception side so as to obtain third signed data;

an eighth step of merging said obtained worked data and said third signed data and applying a one-way function to obtained merged data;

a ninth step of enciphering said received second signed data with a private key of said data transmission side; and

a tenth step of comparing results of said eighth and ninth steps so as to verify data validity.

2. A method according to Claim 1, wherein said recording medium including paper, and said original image is an image of said written information on said paper read out by scanning said paper.

3. A method according to Claim 1, wherein said written information includes a string of characters.

4. A method according to Claim 1, wherein said first signed data in said second step includes signed data obtained by applying a digital signature to data relating to said original image.

5. A method according to Claim 4, wherein said data relating to said original image includes a volume of data of said original image.

6. A method according to Claim 4, wherein said data relating to said original image includes a number

of black pixels included in a binarized image obtained by image-processing said original image.

7. A method according to Claim 1, wherein said data reception side further sends said third signed data obtained in said seventh step to said data transmission side when a comparison result in said tenth step exhibits disagreement between outputs of said eighth and ninth steps; and

said data transmission side searches for an original image corresponding to signed data coinciding with said third signed data sent to the data transmission side.

8. A method for making an electronic exchange of an original image of written information read out of a recording medium between a data transmission side and a data reception side via a network, comprising:

a data transmission step; and

a data reception step;

said data transmission step including:

a first step of applying digital signature to said original image so as to produce first signed data;

a second step of ciphering said first signed data with a private key of said data reception side so as to produce a ciphered signed data;

a third step of merging said original image data and said first signed data, applying a one-way function to obtained merged data, and ciphering an output of said one-way function with a secret key of

said data transmission side so as to obtain second signed data; and

a fourth step of transmitting said original image data, said second signed data and said ciphered signed data to said data reception side;

said data reception step including:

a fifth step of obtaining said original image data, said second signed data and said ciphered signed data;

a sixth step of enciphering said obtained ciphered signed data with a secret key of said data reception side so as to obtain third signed data;

a seventh step of merging said obtained original image data and said third signed data and applying a one-way function to obtained merged data;

an eighth step of enciphering said received second signed data with a private key of said data transmission side; and

a ninth step of comparing results of said steps 8 and 9 so as to confirm data validity.

9. A method according to Claim 8, wherein said recording medium including paper, and said original image is an image of said written information on said paper read out by scanning said paper.

10. A method according to Claim 8, wherein said written information includes a string of characters.

11. A method according to Claim 8, wherein said first signed data in said first step includes signed

data obtained by applying a digital signature to data relating to said original image.

12. A method according to Claim 11, wherein said data relating to said original image includes a volume of data of said original image.

13. A method according to Claim 11, wherein said data relating to said original image includes a number of black pixels included in a binarized image obtained by processing said original image.

14. A method according to Claim 8, wherein said data reception side further sends said third signed data obtained in said sixth step to said data transmission side when a comparison result in said ninth step exhibits disagreement between outputs of said seventh and eighth steps; and

said data transmission side searches for an original image corresponding to signed data coinciding with said third signed data sent to the data transmission side.

15. A data transmission apparatus comprising:

first ciphering means for receiving an electronic image of an original image and a first secret key as inputs, and outputting a first digital signature obtained by ciphering said electronic image with said first secret key;

processing means for receiving said electronic image as input, and outputting a partial or processed image of said electronic image;

second ciphering means for receiving said partial or processed image, said first digital signature and a second secret key as inputs, merging said partial or processed image and said first digital signature, ciphering obtained merged data with said second secret key, and outputting an obtained second digital signature;

third ciphering means for receiving said first digital signature and a private key as inputs, and obtaining ciphered data of said first digital signature with said private key; and

transmitting means for transmitting said partial or processed image, said second digital signature, and said ciphered data of said first signature to an external data channel.

16. A data transmission apparatus according to Claim 15, wherein said first digital signature includes a digital signature obtained by ciphering data relating to said original image with said first secret key.

17. A data transmission apparatus according to Claim 15, wherein said data relating to said original image includes a volume of data of said original image.

18. A data transmission apparatus according to Claim 15, wherein said data relating to said original image includes a number of black pixels included in a binarized image obtained by processing said original image.

19. A data transmission apparatus according to

Claim 15, further comprising a scanner for scanning written paper to thereby produce said electronic image of said original image.